20123670923

intelligence

Ministerial Review Commission on Intelligence
REPUBLIC OF SOUTH AFRICA

PO Box 1037, MENLYN, 0077 Bogare, Cnr Atterbury Road & Lois Avenue, MENLYN
Tel:(012) 367 6700, Fax: (012) 367 0749

MIN/M1/4

11 July 2008

Attention Ms Ntombe Mbuqe
The Secretary to Parliament of the RSA
P.O. Box 15
Cape Town
8000

Dear Ms Mbuqe

SUBMISSION BY THE REVIEW COMMISSION - INTELLIGENCE LEGISLATION ON THE NATIONAL STRATEGIC INTELLIGENCE AMENDMENT BILL (B38-2008)

The Ministerial Review Commission on Intelligence welcomes the call for submissions to the Parliamentary Ad Hoc Committee on Intelligence (National Assembly).

The Commission is pleased to be making a submission to the Ad Hoc Committee on Intelligence. Herewith please find the Review Commission's submission on National Strategic Intelligence Amendment Bill (B38-2008)

Yours Sincerely

Mr J Matthews
Chairperson

Ministerial Review Commission on Intelligence
SUBMISSION ON THE NATIONAL STRATEGIC INTELLIGENCE AMENDMENT BILL [B 38-2008]

10 July 2008

Prepared for the Ad Hoc Committee on Intelligence, National Assembly

1. Introduction

The Ministerial Review Commission on Intelligence has prepared this submission on the National Strategic Intelligence Amendment Bill [B 38-2008] (hereafter "the Bill") for consideration by the Ad Hoc Committee on Intelligence in the National Assembly.

The Commission was established by the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils MP, in 2006. Its members are Joe Matthews (Chairperson), Dr Frene Ginwala and Laurie Nathan. The aim of the Commission's review is to strengthen mechanisms of control of the civilian intelligence structures in order to ensure full compliance and alignment with the Constitution, constitutional principles and the rule of law, and particularly to minimise the potential for illegality and abuse of power.[1]

This submission focuses on the provisions of the Bill that deal with the National Communications Centre (NCC). In February 2008 we submitted to Minister Kasrils a memorandum on an earlier draft of the Bill.[2] The memorandum was based on an opinion we solicited from an advocate in

[1] The Commission's website can be viewed at www.intelligence.gov.za/commission.
[2] Ministerial Review Commission on Intelligence, 'Memorandum on the NCC and Draft NCC Legislation', submitted to the Minister of Intelligence, February 2008.

private practice and on Constitutional Court judgements regarding infringements of the right to privacy.

The Bill that is now before Parliament has been amended in the light of our comments. However, we still have a number of concerns, which we present below. We begin by providing background information on the NCC and then consider the relevant constitutional and legislative provisions.

2. Background on the NCC

The NCC is government's facility for intercepting communication through the monitoring and collection of electronic signals. It monitors the signals of 'targets', being known persons or organisations that have been identified for intelligence monitoring. It also undertakes 'environmental scanning', which entails random monitoring of signals through its bulk monitoring capability.

The formation of the NCC flowed from a proposal by the Pikoli Commission in 1996 that government should establish a single national signals intelligence facility. The aim was to overcome the problem of signals intelligence overlap and duplication among the various intelligence bodies by centralising the state's signals intelligence capacity in a single entity. The NCC's clients are the National Intelligence Agency (NIA), the South African Secret Service (SASS), the South African Police Service (SAPS) and the Financial Intelligence Centre (FIC).

The Bill provides for the functions of the NCC and the manner in which these functions are to be performed. The functions include "to collect and analyse foreign signals intelligence in accordance with the intelligence priorities of the Republic".[3] The Bill defines "foreign signals intelligence" to mean "intelligence

[3] Section 2A(a)(i) of the Bill.

derived from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals, and includes any communication that emanates from outside the borders of the Republic, or passes through or ends in the Republic".[4]

Because the Bill deals with the interception of private communication, it is necessary to assess its provisions in light of the constitutional right to privacy.

3. The Right to Privacy

3.1 Constitutional provisions

The Constitution protects the right to privacy as follows: "Everyone has the right to privacy, which includes the right not to have a) their person or home searched; b) their property searched; c) their possessions seized; or d) the privacy of their communications infringed".[5]

The interception of private communication also infringes the Constitution's provision on dignity, which states that "everyone has inherent dignity and the right to have their dignity respected and protected".[6]

The Bill provides that the NCC may intercept foreign signals that emanate from outside the borders of the country and pass through or end in South Africa. The communication intercepted by the NCC might consequently be sent by a South African who is outside the country and/or it might be received by a South African who is inside the country. The Constitution affords citizens the right to privacy and they enjoy this right in relation to the state even when they are beyond the borders of South Africa.

---

[4] Section 1(b) of the Bill.
[5] Section 14 of the Constitution.
[6] Section 10 of the Constitution.

Further, the constitutional right to privacy is not limited to citizens but applies to every person in South Africa. The Constitutional Court has interpreted other constitutional rights in this fashion where the right, according to the Constitution, is held by "everyone".[7]

Because the Bill allows for infringements of the right to privacy, it must comply with the constitutional provisions on limitation of rights. Section 36(1) of the Constitution states the following in this regard:

> The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including a) the nature of the right; b) the importance of the purpose of the limitation; c) the nature and extent of the limitation; d) the relation between the limitation and its purpose; and e) less restrictive means to achieve the purpose.

The relevant law of general application regarding the interception of communication is the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 (hereafter "RICA"). This Act, discussed below, prohibits the interception of private communication without prior judicial authorisation.

While all intrusive methods used by the state are constitutionally and politically sensitive, the secret use of these methods by intelligence services is especially sensitive because the person under scrutiny is unlikely to ever learn of the investigation. As a result, the targeted person cannot object to the

[7] See *Lawyers for Human Rights v Minister of Home Affairs* 2004 (4) SA 125 (CC); and *Mohamed v President of the Republic of South Africa* 2001 (3) SA 893 (CC).

intrusion and challenge its validity in court. Unable to mount a legal challenge, the person is effectively deprived of his or her rights relating to just administrative action[8] and access to courts.[9]

3.2 *Universal right to privacy*

The Constitution declares that the Republic is bound by international agreements that were binding on South Africa when the Constitution took effect,[10] and that customary international law is law in the Republic unless it is inconsistent with the Constitution or an Act of Parliament.[11]

Article 12 of the Universal Declaration of Human Rights states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[12] This right is repeated in article 17 of the International Covenant on Civil and Political Rights.[13] South Africa is a signatory to the Covenant.

The right to privacy is thus a universal human right that is protected by our Constitution and naturally applies as much to people outside the country as to people inside.

3.3 *The Convention on Cybercrime*

South Africa is a non-member signatory of the Council of Europe's Convention on Cybercrime of 2001.[14] The Convention provides for a range of criminal offences relating to computers and computer data, such as

[8] Section 33 of the Constitution.
[9] Section 34 of the Constitution.
[10] Section 231(5) of the Constitution.
[11] Section 232 of the Constitution.
[12] The Declaration can be viewed at www.un.org/Overview/rights.html.
[13] The Covenant can be viewed at www1.umn.edu/humanrts/instree/b3ccpr.htm.
[14] The Convention can be viewed at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

computer-related fraud and crimes related to child pornography. It states that the signatories shall adopt such legislative and other measures as may be necessary to establish these offences under its domestic law and establish the powers and procedures for criminal investigations and proceedings. The powers and procedures include interception of electronic communication and search and seizure of computer data.

Article 15 of the Convention provides for conditions and safeguards as follows:

> Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, ...and which shall incorporate the principle of proportionality.
>
> Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
>
> To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

3.4 Judgements of the Constitutional Court

The Constitutional Court has interpreted the right to privacy as follows:

> The right [to privacy], however, does not relate solely to the individual within his or her intimate space. ...Thus, when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied. Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play.[15]

Where the Court has been called on to judge the constitutionality of legislation that permits infringements of the right to privacy, it has emphasised the necessity for safeguards to protect this right:

> The existence of safeguards to regulate the way in which state officials may enter the private domains of ordinary citizens is one of the features that distinguish a constitutional democracy from a police state. South African experience has been notoriously mixed in this regard. On the one hand, there has been an admirable history of strong statutory controls over the powers of the police to search and seize. On the other, when it came to racially discriminatory laws and security legislation, vast and often unrestricted discretionary powers were conferred on officials and police. ...[The constitutional right to privacy] requires us to repudiate the past practices that were repugnant to the new constitutional values, while at the same time re-affirming and building on those that are consistent with these values.[16]

In the *Hyundai* case, the Court held that the search and seizure provisions in the National Prosecuting Authority Act No. 32 of 1998 were not unconstitutional. Central to this decision was the Court's assessment that the

---

[15] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others*, 2001 (1) SA 545 (CC), para 16.
[16] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC), para 25.

legislation contained substantial safeguards protecting the right to privacy. The most important safeguard was the necessity to obtain judicial authorisation for search and seizure activities.[17]

4. RICA

In accordance with the constitutional right to privacy, RICA prohibits the interception of private communication. As an exception to this prohibition, it allows a member of an intelligence service, the police service, the defence force and other specified organisations to apply to a designated judge for an interception direction permitting a member of that organisation to intercept a person's communication without the knowledge of that person.

The judge may issue an interception direction for a period of up to three months if he or she is satisfied that the requirements of the Act have been met. A 'designated judge' is a retired judge designated by the Minister of Intelligence for the purposes of this Act.

The Act stipulates the grounds on which the judge may issue an interception order and specifies which of these grounds can be invoked by each of the security services and law enforcement organisations.[18]

An application for an interception order must indicate, *inter alia*, the name of the person, if known, whose communication is to be intercepted; the nature and location of the facilities, if known, from which the communication is to be intercepted; the grounds on which the application is made; and the basis for believing that evidence relating to the grounds on which the application is

[17] *Investigating Directorate v Hyundai*, op cit.
[18] Sections 16(3) and 16(5) of RICA.

made will be obtained through the interception.[19] The application must also indicate whether other investigative procedures have been applied and failed to produce the required evidence or must indicate the reason why other investigative procedures reasonably appear unlikely to succeed or are too dangerous to apply in order to obtain the required evidence.[20]

RICA regards the interception of communication as a method of last resort. Before issuing an interception order, the judge must be satisfied "that other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner".[21]

5. The Bill's Provisions on the NCC

In this final section we raise six concerns about the Bill's provisions on the NCC.

5.1 Who can make use of the NCC?

As noted in section 2 above, the NCC's clients currently include NIA, SASS, the SAPS and the FIC. However, the Bill does not state that these bodies (or any other bodies) are entitled to make use of the NCC. Given the sensitivity of both intelligence gathering and infringing the right to privacy, the Bill should

[19] Section 16(2) of RICA.
[20] Section 16(2)(e) of RICA.

specify who is entitled to apply to the NCC for assistance with the interception of communications. RICA provides a good example in this regard.[22]

In relation to the above, it is unclear whether the NCC can on its own initiative identify a target for signals monitoring or whether the NCC can only monitor the targets identified by another intelligence service or a law enforcement body. The Bill ought to provide clarity on this matter.

5.2 What information is required in an application to monitor signals?

As noted in section 4 above, RICA specifies in detail the information that must be provided in an application to intercept communication. This helps to reduce the potential for mischief and prevent inappropriate and unjustified infringements of privacy. The Bill should similarly indicate the information that must be contained in an application for signals monitoring.

5.3 What is the NCC's relationship to RICA?

The NCC's relationship to RICA is unclear. The uncertainty arises from section 2(A)(a)(i) of the Bill, which states that the Inspector-General of Intelligence must report annually to Parliament on the NCC's activities and in such report must indicate any contraventions by the NCC of the provisions of RICA. However, the Bill does not state the manner in which the NCC is bound by RICA. If the Inspector-General is to monitor the NCC's compliance with its obligations under RICA, then these obligations ought to be spelt out clearly in the Bill.

We recommend that the following addition be made to the Bill: "The NCC may not intercept foreign signals, whether on its own initiative or at the request of a law enforcement body or security service, unless it has obtained in respect

[22] Sections 16(3) and 16(5) of RICA.

of the specified target or communication an interception direction issued by the designated judge as provided for in RICA".

5.4 On what grounds can the NCC intercept communication?

Two of the grounds on which the Bill permits the interception of communication are too broad. These grounds are a) the protection and advancement of international relations and the economic well-being of the Republic;[23] and b) support for preventing and detecting regional and global hazards and disasters that threaten life, property and the environment.[24]

From a constitutional perspective, the broadness of these grounds creates doubt that they can reasonably be invoked to infringe the right to privacy. They would allow for eavesdropping by the state not only in relation to major security threats and criminal offences but also in relation to private activities and conversations that are lawful. They would permit, for example, the secret interception of the communication of bankers, economists and traders if this were deemed to advance the economic well-being of the country.

In relation to search and seizure, South African courts have long maintained a "jealous regard for the liberty of the subject and his or her rights to privacy and property".[25] There is no reason to believe that the courts would view the electronic interception of communication any differently.

5.5 A matter of last resort

Given the constitutional right to privacy, the state may not intercept private communication routinely and lightly. Infringements of this right must be a matter of last resort when non-intrusive means are unable to achieve a

[23] Section 2(A)(b)(ii) of the Bill.
[24] Section 2(A)(b)(iv) of the Bill.
[25] *Powell NO v Van der Merwe NO* 2005 (5) SA 62 (SCA), para 59.

legitimate objective. As in the case of RICA, the Bill should provide that interception of communication is a matter of last resort.

5.6 What happens to incidental information?

The interception of communication by intelligence services might uncover intimate personal information that has nothing to do with the security of the country or the purpose of the investigation. The Bill must therefore provide for the discarding of this personal information.